MTH4104 **Introduction to Algebra**

Extra questions for chapter 3 **Spring 2021**

These questions are for you to practice with on your own schedule. You may e.g. want to try some each week as their topics come up in lectures, or use them in exam revision.

3 Algebraic structures

3.1 Rings and fields

I have combined this section and the following into a single list of questions in this document.

3.2 Understanding the axioms

Question 3.2.1 Let $m \geq 2$ be an integer.

(a) Prove that the set $m\mathbb{Z} := \{mk : k \in \mathbb{Z}\}$ is a ring, with the usual definitions of addition and multiplication on the integers.

[This question does not take as much work as it seems, because $m\mathbb{Z}$ is a subset of $\mathbb{Z}$. This means that some of the ring axioms for $m\mathbb{Z}$ follow immediately from the corresponding axiom for $\mathbb{Z}$. Look out for these.]

(b) Prove that $m\mathbb{Z}$ is not a ring with identity.

["$1 \notin m\mathbb{Z}$" is *not* a proof by itself! Remember that the "1" in the law can stand for any element of the ring.]

Solution To prove something is a ring, we need to prove all of the ring axioms. Let's start doing that and see how it goes.

Additive closure law. We must prove that if a and b are elements of $m\mathbb{Z}$, then $a+b \in m\mathbb{Z}$. Let $a = km$ and $b = lm$ for integers k and l. Then $a+b = (k+l)m$ is a multiple of m, so it is in $m\mathbb{Z}$ as needed.

Multiplicative closure law. Similarly, we must prove that if a and b are elements of $m\mathbb{Z}$, then $ab \in m\mathbb{Z}$. Indeed, if $a = km$ and $b = lm$ for integers k and l then $ab = klm^2 = (klm)m \in m\mathbb{Z}$.

Additive associative law. We must prove that if a, b and c are elements of $m\mathbb{Z}$, then $(a+b)+c = a+(b+c)$. But a, b, and c are just (certain special) integers, and we know that $(a+b)+c = a+(b+c)$ for all integers a, b, and c. That's it—there's nothing else to prove!

This is the situation the hint in the question was talking about. The same situation will arise whenever the law that we need to prove is that some equation holds for all elements $a, b, \ldots$ in the ring. The multiplicative associative law, the additive commutative law, and the distributive law are also like this. So we get these laws "for free" just as we got the additive associative law for free above.

Additive identity law. We do not quite get this for free, because we have to prove that there exists a zero element *in* $m\mathbb{Z}$, and what we know about the integers just says that there is a zero element in $\mathbb{Z}$. But clearly $0 = 0m$ is a multiple of m, so $0 \in m\mathbb{Z}$. And now we do get the *equation* that is the payload of the law for free: for any $a \in m\mathbb{Z}$, it is true that $0+a = a+0 = a$, because this is true for integers. So 0 is the zero element in $m\mathbb{Z}$.

Additive inverse law. Similarly to the last law, the part we have to prove is that if $a \in m\mathbb{Z}$ then $-a \in m\mathbb{Z}$. This is indeed true, because if $a = km$ then $-a = (-k)m$. Now $a+(-a) = (-a)+a = 0$ is true because this is true for integers.

We conclude that $m\mathbb{Z}$ is a ring.

(b) As stated in the hint, what we need to prove is that there is no element $e \in m\mathbb{Z}$ such that $ea = ae = a$ for all $a \in m\mathbb{Z}$.

We proceed by contradiction. Suppose there was such an element $e \in m\mathbb{Z}$. We may take $a = m$, which is an element of $m\mathbb{Z}$, in the multiplicative identity law, which gives us $em = m$. This is now an equation in $\mathbb{Z}$ so the gloves are off, and we can handle it using everything we know about integers and other familiar kinds of numbers. Since m is nonzero, we can divide through by m in the equation $em = m$; this moves the equation into the rational numbers, but that is not a problem. This implies $e = 1$ (as we suspected all along). But 1 is not a multiple of m, so $e = 1$ is not an element of $m\mathbb{Z}$, which is the contradiction sought.

Question 3.2.2 Let X be a non-empty set and let $S = \mathscr{P}(X)$ be the set of all its subsets. Define operations of addition and multiplication on S by the rules

$$A + B := (A \cup B) \setminus (A \cap B)$$

and

$$AB := A \cap B$$

for any $A, B \in S$.

(a) Prove that S is a ring.

[I will accept Venn diagram "proofs", but if you do this, please still use full sentences to explain your argument. In your proofs, you should be exceedingly clear which elements you have selected as the identity elements ("0" and "1").]

(b) Is S a ring with identity? a skewfield? a commutative ring?

Solution (a) We must prove all of the ring axioms.
Associativity of addition. Let $x \in X$. Then

$$\begin{aligned} & x \in A+(B+C) \\ \iff & x \in A, x \notin (B+C) \text{ or } x \notin A, x \in (B+C) \\ \iff & x \in A, (x \in B, x \in C \text{ or } x \notin B, x \notin C) \text{ or } x \notin A, (x \in B, x \notin C \text{ or } x \notin B, x \in C) \end{aligned}$$

whereas

$$\begin{aligned} & x \in (A+B)+C \\ \iff & x \in (A+B), x \notin C \text{ or } x \notin (A+B), x \in C \\ \iff & (x \in A, x \notin B \text{ or } x \notin A, x \in B), x \notin C \text{ or } (x \in A, x \in B \text{ or } x \notin A, x \notin B), x \in C \end{aligned}$$

and these are the same condition. (Commas mean "and" here, to save space.)
Additive identity. The additive identity is $\emptyset$. Indeed

$$A+\emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A.$$

(And because addition is commutative I don't have to do the other side.)
Additive inverse. Every set A is its own additive inverse. Indeed

$$A+A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset,$$

and $\emptyset$ is the additive identity.
Commutativity of addition. $\cup$ and $\cap$ are both commutative, hence so is $+$:

$$A+B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B+A.$$

Associativity of multiplication. This follows because $\cap$ is associative:

$$\begin{aligned} & x \in A(BC) \\ \iff & x \in A \text{ and } x \in BC \\ \iff & x \in A \text{ and } x \in B \text{ and } x \in C \\ \iff & x \in AB \text{ and } x \in C \\ \iff & x \in (AB)C. \end{aligned}$$

Distributivity.

$$\begin{aligned} & x \in A(B+C) \\ \iff & x \in A, x \in B+C \\ \iff & x \in A, (x \in B, x \notin C \text{ or } x \notin B, x \in C) \end{aligned}$$

whereas

$$\begin{aligned} & x \in AB+AC \\ \iff & x \in AB, x \notin AC \text{ or } x \notin AB, x \in AC. \end{aligned}$$

Now if $x \in AB$ then $x \in A$ and $x \in B$. But if also $x \notin AC$ then at least one of $x \in A$ and $x \in C$ has to be false; but $x \in A$ so it must be that $x \notin C$. Therefore the condition before the "or" here is equivalent to the condition before the "or" in the first display. A similar argument shows that the conditions after the "or" are equivalent too. So these sets are the same.

I also have to prove that $(A+B)C = AC+BC$, but the efficient[1] way to do this is to invoke commutativity of multiplication from part (d). In a commutative ring the two parts of the distributive law are equivalent, as you can swap round the products.

(b) S is a ring with identity. The multiplicative identity is X, as for any $A \in S$,

$$AX = A \cap X = A$$

because A is a subset of X. Similarly $XA = X$.

S is a skewfield if $|X| = 1$, and is not if $|X|$ is larger. First suppose X has at least two elements, and let x be one of them. Then $\{x\} \in S$ is nonzero but has no multiplicative inverse, because there is no set whose intersection with $\{x\}$ is the larger set X. If however $|X| = 1$, then the only subsets of X are $\emptyset$ and X. The former is not supposed to have a multiplicative inverse, and the latter is its own multiplicative inverse.

S is a commutative ring, because $\cap$ is commutative.

Question 3.2.3 Give an example of a ring that is neither commutative nor a ring with identity. Justify your answer. You need not give a complete proof, but you should give

(a) a counterexample to the commutative law for multiplication;

(b) an proof that your ring contains no multiplicative identity element;

(c) a general reason for why the ring axioms are true. This can be short but, as always, should be in complete sentences.

[Hint: try to "build" your example from rings you have seen with useful properties in the notes or other module material. If you have not yet seen an example of a non-commutative ring, come back to this question after you have.]

Solution There are lots of examples; here's one.

In lecture I mentioned that an example of a ring without identity is the set of even integers

$$2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}.$$

(Indeed you could use multiples of any integer greater than 1, not just 2.) This doesn't solve the problem by itself, as $2\mathbb{Z}$ is commutative. But perhaps we can build a noncommutative ring from it?

I also mentioned that matrix rings are usually not commutative, so perhaps a matrix ring over $2\mathbb{Z}$ will give us our example. This indeed works. To be concrete, let's show that $\mathrm{M}_2(2\mathbb{Z})$ is a noncommutative ring without identity.

(a) A counterexample to the commutative law for multiplication in $\mathrm{M}_2(2\mathbb{Z})$ is given by

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2\cdot 0+0\cdot 0 & 2\cdot 2+0\cdot 0 \\ 0\cdot 0+0\cdot 0 & 0\cdot 2+0\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}$$

[1] For "efficient", read "lazy". It's fine with me if your own proofs are similarly efficient.

which is not equal to

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0\cdot 2+2\cdot 0 & 0\cdot 0+2\cdot 0 \\ 0\cdot 2+0\cdot 0 & 0\cdot 0+0\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(b) Nor does $\mathrm{M}_2(2\mathbb{Z})$ satisfy the multiplicative identity law. Indeed, in any product of two matrices in this ring, say

$$\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} \cdot \begin{pmatrix} 2e & 2f \\ 2g & 2h \end{pmatrix} = \begin{pmatrix} 4(ae+bg) & 4(af+bh) \\ 4(ce+dg) & 4(cf+dh) \end{pmatrix}$$

for integers a,b,c,d,e,f,g,h, every entry of the product is a multiple of 4. Therefore, since 2 is not a multiple of 4, there is no matrix in $\mathrm{M}_2(2\mathbb{Z})$ whose product with $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$ will be $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$ again.

(c) $\mathrm{M}_2(2\mathbb{Z})$ is a ring by facts from lectures, since we argued that $2\mathbb{Z}$ is a ring last week, and $\mathrm{M}_n(R)$ is a ring for any ring R and integer $n \geq 1$.

3.3 The complex numbers

Question 3.3.1 Find the real and imaginary parts of $\dfrac{-3+5\mathrm{i}}{2-9\mathrm{i}}$.

Solution To calculate a ratio of complex numbers z/w in the standard form $a+b\mathrm{i}$ with a,b real, we can still use our old method for removing surds from the denominator:

$$\frac{z}{w} = \frac{z\bar{w}}{w\bar{w}} = \frac{z\bar{w}}{|w|^2}.$$

Thus

$$\frac{-3+5\mathrm{i}}{2-9\mathrm{i}} = \frac{(-3+5\mathrm{i})(2+9\mathrm{i})}{(2-9\mathrm{i})(2+9\mathrm{i})} = \frac{-6-27\mathrm{i}+10\mathrm{i}+45\mathrm{i}^2}{2^2+9^2} =$$

$$= \frac{-6-45}{85} + \frac{-27+10}{85}\cdot\mathrm{i} = \frac{-51}{85} + \frac{-17}{85}\mathrm{i} = -\frac{3}{5} - \frac{1}{5}\mathrm{i}.$$

The real and imaginary parts of this fraction are, respectively, $-3/5$ and $-1/5$.

If you're thinking of our workings in lecture which proved the multiplicative inverse law for the complex numbers, they provide another approach to questions like this. You could expand the product on the left hand side in

$$(a+b\mathrm{i})(2-9\mathrm{i}) = 3+5\mathrm{i},$$

equate the real and complex parts of the left and right hand sides, and obtain two linear equations to solve in the two real numbers a and b. But this is not a *superior* method to the one above; it's just the one provided to us by the field axioms if we happened not to remember other facts about the complex numbers. Both methods would reach the same answer.

Question 3.3.2 Solve the linear equation

$$3(1-\mathrm{i})z-2=2z+\mathrm{i}+1.$$

Include a check that your answer is correct.

Solution Because $\mathbb{C}$ is a field, all of the steps we usually use in solving a linear equation are valid in it. So we can solve linear equations as we are used to.

The first step is to collect the linear and constant terms each together.

$$\begin{aligned} & 3(1-\mathrm{i})z-2=2z+\mathrm{i}+1 \\ \implies\quad & (3-3\mathrm{i}-2)z=\mathrm{i}+1+2 \\ \implies\quad & (-3\mathrm{i}+1)z=\mathrm{i}+3 \\ \implies\quad & z=\frac{3+\mathrm{i}}{-3\mathrm{i}+1}. \end{aligned}$$

The first step uses the inverse law for addition, after adding the same quantity to both sides, as well as the distributive law to collect z on the left. The second step just uses the definition of addition in $\mathbb{C}$. The third uses the definition of multiplicative inverse, as well as the notation x/y meaning xy^{-1} (in a commutative ring).

We can now use the standard procedure for complex division, but it's quicker to spot that

$$z=\frac{3+\mathrm{i}}{-3\mathrm{i}+1}=\frac{3+\mathrm{i}}{-3\mathrm{i}-\mathrm{i}^2}=\frac{3+\mathrm{i}}{-(3+\mathrm{i})\mathrm{i}}=\frac{1}{-\mathrm{i}}=\mathrm{i}.$$

To check that this answer is correct, we substitute $z=\mathrm{i}$ into the original equation

$$3(1-\mathrm{i})\mathrm{i}-2=3\mathrm{i}-3\mathrm{i}^2-2=3\mathrm{i}+1=2\mathrm{i}+\mathrm{i}+1$$

and see that it is satisfied.

Question 3.3.3 Write up careful proofs of all of the field axioms for $\mathbb{C}$.

Solution I'm afraid I haven't actually written this proof out completely. As examples, I will write out proofs of two more of the axioms here that are not treated in the notes. The rest follow similar patterns. I encourage you to write them all out, and email me if you're unsure of something and would like me to check.

Inverse law for addition. In lectures, we showed that the additive identity element for the complex numbers is $0+0\mathrm{i}$. So, given a complex number x, we must prove that there exists a complex number y such that $x+y=y+x=0+0\mathrm{i}$. If $x=a+b\mathrm{i}$ where a and b are real, then we may take $y=-a-b\mathrm{i}$ because

$$x+y=(a+b\mathrm{i})+(-a-b\mathrm{i})=(a+(-a))+(b+(-b))\mathrm{i}=0+0\mathrm{i}$$

and

$$y+x=(-a-b\mathrm{i})+(a+b\mathrm{i})=(-a+a)+(-b+b)\mathrm{i}=0+0\mathrm{i}.$$

Associative law for multiplication. We must prove that for all $u,v,w\in\mathbb{C}$, the equation

$$(uv)w=u(vw)$$

holds. Write the given complex numbers $u = a+b\mathrm{i}$, $v = c+d\mathrm{i}$, $w = e+f\mathrm{i}$ where a through f are real. Then

$$\begin{aligned}(uv)w &= ((a+b\mathrm{i})(c+d\mathrm{i}))(e+f\mathrm{i}) = ((ac-bd)+(ad+bc)\mathrm{i})(e+f\mathrm{i}) = \\ &= (ac-bd)e-(ad+bc)f+((ac-bd)f+(ad+bc)e)\mathrm{i} = \\ &= (ace-bde-adf-bcf)+(acf-bdf+ade+bce)\mathrm{i}\end{aligned}$$

whereas

$$\begin{aligned}u(vw) &= (a+b\mathrm{i})((c+d\mathrm{i})(e+f\mathrm{i}) = (a+b\mathrm{i})((ce-df)+(cf+de)\mathrm{i}) = \\ &= a(ce-df)-b(cf+de)+(a(cf+de)+b(ce-df))\mathrm{i} = \\ &= (ace-adf-bcf-bde)+(acf+ade+bce-bdf)\mathrm{i}.\end{aligned}$$

The two expressions are equal since addition of real numbers is commutative.

Question 3.3.4 If $z = a+b\mathrm{i}$ is a complex number, then its *conjugate* is defined to be $\overline{z} = a-b\mathrm{i}$.

(a) Prove that, if z and w are complex numbers, then $\overline{z}+\overline{w} = \overline{z+w}$ and $\overline{z}\cdot\overline{w} = \overline{zw}$.

(b) Prove that also $\overline{z}-\overline{w} = \overline{z-w}$ and, if w is nonzero, $\overline{z}/\overline{w} = \overline{z/w}$.

If you've done part (a), you could do this part similarly, by imitating that proof. Can you see, instead, how to *use* part (a) to prove this with less tedium?

(c) If you take any arithmetic expression in complex numbers, and transform it by replacing every number in it by its conjugate, the transformed expression evaluates to the conjugate of the value of the original expression. Write up a clear explanation of why this is true, in view of parts (a) and (b).

Solution (a) This is another routine proof like most of the proofs of the field axioms. Expanding in standard form, let $z = a+bi$ and $w = c+di$ where a, b, c, and d are real numbers. To prove $\overline{z}+\overline{w} = \overline{z+w}$ we substitute into and expand each side. On the left we have

$$\overline{z}+\overline{w} = \overline{a+bi}+\overline{c+di} = a-bi+c-di = (a+c)+(-b-d)i$$

whereas on the right, we have the conjugate of

$$z+w = a+bi+c+di = (a+c)+(b+d)i,$$

which we form by negating the imaginary part, yielding $(a+c)+(-b-d)i$. The two results are equal, so the proof of $\overline{z}+\overline{w} = \overline{z+w}$ is complete.

To prove $\overline{z}\cdot\overline{w} = \overline{zw}$ we proceed similarly. On the left we have

$$\overline{z}\cdot\overline{w} = \overline{a+bi}\cdot\overline{c+di} = (a-bi)\cdot(c-di) = (ac-(-b)(-d))+(a(-d)+b(-c))i.$$

On the right, we have the conjugate of

$$zw = (a+bi)(c+di) = (ac-bd)+(ad+bc)i,$$

which is $(ac-bd)+(-ad-bc)i$. This is, again, the same result we got on the left hand side, so we have proved that $\overline{z}\cdot\overline{w}=\overline{zw}$.

(b) In part (a) we proved that $\overline{z}+\overline{w}=\overline{z+w}$ and $\overline{z}\cdot\overline{w}=\overline{zw}$ by expanding into real and imaginary parts. You can also prove in the same way that $\overline{z}-\overline{w}=\overline{z-w}$ and $\overline{z}/\overline{w}=\overline{z/w}$. And that's a fine way to do it; after all, the computations aren't much work. But you could also prove it as a corollary of part (a) without doing the expansion again. For example, for division, first observe that since

$$\overline{w}\cdot\overline{w^{-1}}=\overline{ww^{-1}}=\overline{1}=1$$

we have $\overline{w^{-1}}=1/\overline{w}$, and therefore

$$\overline{z/w}=\overline{zw^{-1}}=\overline{z}\cdot\overline{w^{-1}}=\overline{z}\cdot(1/\overline{w})=\overline{z}/\overline{w}.$$

For subtraction a similar argument holds.

(c) We will go one better than a clear explanation, and give a proof.

I haven't defined "arithmetic expression", so I'd be happy with any reasonable interpretation of this phrase But certainly any calculation performed via a sequence of additions, subtractions, multiplications, and divisions should count as such an expression.

So what we want to prove is that given any algebraic expression made of any number of additions, subtractions, multiplications, and divisions, if you conjugate each complex number in it, the effect is to conjugate the final answer. This can be proved by mathematical induction! Let $P(n)$ be the statement that our claim about conjugation is true for any expression with up to n operations (namely $+$, $-$, $\cdot$, or $/$) in it. We take $P(1)$ as a base case. This we have proved in the foregoing discussion, because an expression with one operation looks like $z+w$ or $z-w$ or zw or z/w.

Now, let us assume $P(k)$ is true and try to prove $P(k+1)$. The hypothesis of $P(k+1)$ is that we have an algebraic expression with $k+1$ operations in it. Let's say that the expression evaluates to some result r. Focus on one of the operations in it which can be done first: for example, if our expression were

$$\frac{a+bc}{d-e}$$

where $a,\ldots,e$ were complex numbers, then one way we could start evaluating it is by multiplying out b times c. Let us use the notation "$z*w$" for this first subcomputation, where z and w are the complex number arguments, and $*$ stands for $+$, $-$, $\cdot$, or $/$. By the above argument, $\overline{z}*\overline{w}=\overline{z*w}$.

Therefore, if we consider evaluating our expression after conjugating all the complex numbers in it, the first thing we will do is compute $\overline{z}*\overline{w}$, getting $\overline{z*w}$. If we substitute this intermediate result $\overline{z*w}$ into our expression but leave the rest unevaluated, we have a new expression with only k operations left in it, in which all the complex numbers have been conjugated. By the inductive hypothesis, the final value of this new expression is $\overline{r}$. But this is what was to be shown, so our proof by induction is complete.

If your notion of "algebraic calculation" included other operations, like extraction of roots, I encourage you to expand this proof to encompass them.

Commentary. The point of this question is that conjugation is a *symmetry* of the complex numbers. As John H. Conway, whom you may know for inventing the Game of Life, put it:

> [T]here is no property enjoyed by i which is not shared by $-i$. In fact we reply to questions about "the square root of -1" by simply asking exactly which square root of -1 is meant?

In later modules in algebra, when you study *isomorphisms* between algebraic structures, you will see how symmetries like this can be put on a rigorous footing.

Question 3.3.5 Define addition and multiplication operations on the set $U = \mathbb{R}^2$ by

$$\begin{aligned}(a,b)+(c,d) &= (a+c,\, b+d),\\ (a,b)\cdot(c,d) &= (ac,\, ad+bc).\end{aligned}$$

(a) Name the multiplicative identity element in U, and prove the multiplicative identity law.

(b) Prove that, if $a \neq 0$, then (a,b) has a multiplicative inverse in U.

Solution (a) The multiplicative identity element is $(1,0)$, because by definition

$$(a,b)\cdot(1,0) = (1a,\, 0a+1b) = (a,b)$$

and

$$(1,0)\cdot(a,b) = (1a,\, 1b+0a) = (a,b).$$

(b) An inverse of (a,b) under this assumption is $(1/a, -b/a^2)$, which under the assumption $a \neq 0$ is well-defined. To verify that it is an inverse we compute

$$\begin{aligned}(a,b)\cdot(\frac{1}{a},\frac{-b}{a^2}) &= (a\frac{1}{a},\, a\frac{-b}{a^2}+b\frac{1}{a})\\ &= (\frac{a}{a},\frac{-ab+ab}{a^2})\\ &= (1,0)\end{aligned}$$

and

$$\begin{aligned}(\frac{1}{a},\frac{-b}{a^2})\cdot(a,b) &= (\frac{1}{a}a,\, \frac{1}{a}b+\frac{-b}{a^2}a,)\\ &= (\frac{a}{a},\frac{ba-ba}{a^2})\\ &= (1,0).\end{aligned}$$

Question 3.3.6 Let U be the set of expressions of the form $a+bu$ where a and b are real numbers. The u is a formal symbol. We want to make U into a ring similar to how we defined $\mathbb{C}$ as a ring, and we'd like u to satisfy the equation $u^2 = 2u-2$.

(a) Provide the formulas we should use to define $+$ and $\cdot$ in U.

(b) Using your definitions, prove in U:

  (i) the identity laws for addition and multiplication;

  (ii) the associative law for multiplication.

(c) Is the inverse law for multiplication true in U?

Solution (a) If U is to satisfy the commutative and associative and distributive laws, then we can add and multiply in U just the same way we normally would, treating u as an inert symbol, unless a u^2 appears.

Like it is in $\mathbb{C}$, addition is just a matter of adding corresponding components:

$$(a+bu)+(c+du)=(a+c)+(b+d)u.$$

For multiplication we use distributivity and the fact that $u^2=2u-2$:

$$\begin{aligned}(a+bu)\cdot(c+du)=ac+adu+bcu+bdu^2=ac+(ad+bc)u+bd(2u-2)=\\ =(ac-2bd)+(ad+bc+2bd)u.\end{aligned}$$

Of course, for purposes of writing down a definition of U, we wouldn't have to—indeed, shouldn't—show the intermediate steps; it would be better to write

$$(a+bu)\cdot(c+du):=(ac-2bd)+(ad+bc+2bd)u.$$

(b) The guideline we've used to construct U in part (a) suggests that the real numbers make up a subset of U in the guise of the elements $a+0u$. That suggests trying $0+0u$ for the additive identity element and $1+0u$ for the multiplicative identity element. Indeed, those work. Using the definitions from port (a) we verify these, getting

$$(a+bu)+(0+0u)=(a+0)+(b+0)u=a+bu$$

and

$$(0+0u)+(a+bu)=(0+a)+(0+b)u=a+bu$$

for addition, and

$$(a+bu)\cdot(1+0u)=(a1-2b0)+(a0+b1+2b0)u=a+bu$$

and

$$(1+0u)\cdot(a+bu)=(1a-2\cdot 0b)+(1b+0a+2\cdot 0b)=a+bu$$

for multiplication.

For the associative law for multiplication, we take three elements $a+bu$, $c+du$, $e+fu$ of U, and compare the two products

$$\begin{aligned}&\big((a+bu)(c+du)\big)(e+fu)\\ &=\big((ac-2bd)+(ad+bc+2bd)u\big)(e+fu)\\ &=((ac-2bd)e-2(ad+bc+2bd)f)+((ac-2bd)f+(ad+bc+2bd)e+2(ad+bc+2bd)f)u\\ &=(ace-2adf-2bcf-2bde-4bdf)\\ &\qquad+(acf+ade+2adf+bce+2bcf+2bde+2bdf)u\end{aligned}$$

and

$$\begin{aligned}&(a+bu)\big((c+du)(e+fu)\big)\\ &=(a+bu)\big((ce-2df)+(cf+de+2df)u\big)\\ &=(a(ce-2df)-2b(cf+de+2df))+(a(cf+de+2df)+b(ce-2df)+2b(cf+de+2df))u\\ &=(ace-2adf-2bcf-2bde-4bdf)\\ &\qquad+(acf+ade+2adf+bce+2bcf+2bde+2bdf)u.\end{aligned}$$

These are equal, so the associative law for multiplication holds.

Again, the few axioms I named in the question are just a selection. It turns out U is a commutative ring with identity, and you could prove the rest of these axioms. Indeed, part (c) will show U is a field.

(c) What the multiplicative inverse law asks is whether, for each element $a+bu \in U$ not equal to $0+0u$ (the additive identity found above), there is another element $c+du$ such that $(a+bu)(c+du) = 1+0u$ (the multiplicative identity found above).

For want of any insight (a counterexample? a familiar way to get the inverse?) let's consider the goal. When we expand out the product

$$(a+bu)(c+du) = (ac-2bd)+(ad+bc+2bd)u$$

we must get $1+0u$; that is, we must have

$$\begin{aligned} ac-2bd &= 1, \\ ad+bc+2bd &= 0. \end{aligned}$$

We want to know whether real numbers c and d exist that satisfy these equations, treating a and b as given. So we can try to *solve* for c and d.

To use the method you're familiar with, first we'd isolate a variable, say c in the second equation:

$$c = \frac{-a-2b}{b}d.$$

Ah, we've had to divide by b, so this won't work if b is zero; we'll have to remember to come back to this case. Now substituting this into the first equation gives

$$a\frac{-a-2b}{b}d - 2bd = 1,$$

i.e.

$$d = \frac{1}{a\frac{-a-2b}{b}-2b} = \frac{b}{a(-a-2b)-2b^2} = \frac{-b}{2(\frac{1}{2}a+b)^2+\frac{1}{2}a^2}$$

where my point in completing the square in the last denominator was to show that it is not zero unless $\frac{1}{2}a+b = a = 0$, that is unless $a=b=0$, which we have assumed is not the case. So we can press on and substitute back in for c:

$$c = \frac{-a-2b}{b}\cdot\frac{-b}{2(\frac{1}{2}a+b)^2+\frac{1}{2}a^2} = \frac{a+2b}{2(\frac{1}{2}a+b)^2+\frac{1}{2}a^2}$$

That seems to work, but to be sure, let's plug it back in to our product. I'll write $\Delta = a^2+2ab+2b^2$ for the common denominator just to keep the equation compact:

$$\begin{aligned} (a+bu)(c+du) &= (a+bu)\left(\frac{a+2b}{\Delta}+\frac{-b}{\Delta}u\right) \\ &= \left(a\frac{a+2b}{\Delta}-2b\frac{-b}{\Delta}\right)+\left(a\frac{-b}{\Delta}+b\frac{a+2b}{\Delta}+2b\frac{-b}{\Delta}\right)u \\ &= \frac{a^2+2ab+2b^2}{\Delta}+\frac{-ab+ab+2b^2-2b^2}{\Delta}u \\ &= 1+0u. \end{aligned}$$

So we found a multiplicative inverse! Well, to be precise, we also need to check that $(c+du)(a+bu) = 1+0u$. But since multiplication is commutative in U (proof left to the reader), this product must be the same as the one we have just worked out.

Finally, we have to address the case $b = 0$. But it turns out that the formula for the inverse we found,

$$c+du = \frac{a+2b}{\Delta} + \frac{-b}{\Delta}u,$$

works even if $b = 0$ (so long as a isn't also zero simultaneously). So there is no problem here.

We conclude that the multiplicative inverse law *is* true of U.

Could we have come to this conclusion without all that work? Yes: here's a way. Perhaps you wondered at some point "but what **is** this u? We already have a number that satisfies $u^2 - 2u + 2 = 0$: it's

$$\frac{2 \pm \sqrt{(-2)^2 - 4 \cdot 1 \cdot 2}}{2} = 1 \pm \mathrm{i}\,."$$

If you pick either sign, say $1+\mathrm{i}$, and replace every u with $1+\mathrm{i}$, you'll see that U becomes

$$\{a + b(1+\mathrm{i}) : a, b \in \mathbb{R}\}$$

which it's not too hard to check is all of $\mathbb{C}$, and that when you set $u = 1+\mathrm{i}$ in the definitions of addition and multiplication from (a), they also become the same as the definitions from $\mathbb{C}$. In other words, U was just $\mathbb{C}$ in disguise all along! And $\mathbb{C}$ satisfies the multiplicative inverse law, hence so must U.

This idea of showing two different-looking structures are really the same is pervasive in algebra. The formal way to prove something like this is using a bijection between the two sets. Such a bijection is called an *isomorphism*, and you will meet many isomorphisms if you continue with studies in algebra.

3.4 Rings from modular arithmetic

Question 3.4.1 Write up a complete proof that $\mathbb{Z}_m$ is a commutative ring with identity, where $m > 0$ is an integer.

Solution Like for $\mathbb{C}$, I haven't actually written all these out myself. Email me if you need help. Here, for an example, is the multiplicative identity law.

We must find an element $e \in \mathbb{Z}_m$ — or $1_{\mathbb{Z}_m}$, to use the notation of lectures — such that, for all $x \in \mathbb{Z}_m$, the equation $ex = x = xe$ holds. Given that the multiplicative identity element in $\mathbb{R}$, $\mathbb{Z}$, etcetera is the number 1, probably $e = [1]_m$ will be the correct choice for $\mathbb{Z}_m$. Let us check this. We may now write $x = [a]_m$ for some integer a. Then

$$ex = [1]_m[a]_m = [1 \cdot a]_m = [a]_m = x$$

and

$$xe = [a]_m[1]_m = [a \cdot 1]_m = [a]_m = x,$$

using the definition of multiplication in $\mathbb{Z}_m$.

Question 3.4.2 Let F be the set $\{a+bI : a,b \in \mathbb{Z}_3\}$, where I is a formal symbol. Define operations of addition and multiplication on F by

$$(a+bI)+(c+dI) = (a+c)+(b+d)I,$$
$$(a+bI)\cdot(c+dI) = (ac-bd)+(ad+bc)I.$$

These definitions are meant to make I behave like a square root of $[-1]_3$.

(a) How many elements does F have?

(b) Prove the left distributive law in F.

(c) Name the additive identity element in F, and prove the additive identity law.

(d) Prove the multiplicative inverse law in F.

Like Question 1, F is in fact a field, and you could prove the other axioms if you wanted more practice. Of all the field axioms, the multiplicative inverse law (part (d)) is the one most different from the complex numbers.

(e) Can you interpret F as a set of congruence classes for a relation in some ring, the way $\mathbb{Z}_3$ is a set of congruence classes for a relation on $\mathbb{Z}$, with addition and multiplication defined in the analogous way?

Solution (a) The cardinality of F is $3^2 = 9$. Because $\mathbb{Z}_3$ has three elements, there are three choices for a, and three choices for b, and therefore 3×3 elements altogether. Or to say the same thing in a slightly more formal way, you can put aside the $a+bI$ notation and just regard the elements of F as being ordered pairs (a,b), in which case F is the cartesian product $(\mathbb{Z}_3)^2$, whose cardinality is $3^2 = 9$ by the formula for the cardinality of a cartesian product.

Here are all 9 elements:

$$\begin{aligned} \text{F} = \{\ & [0]_3+[0]_3 I, \quad [1]_3+[0]_3 I, \quad [2]_3+[0]_3 I, \\ & [0]_3+[1]_3 I, \quad [1]_3+[1]_3 I, \quad [2]_3+[1]_3 I, \\ & [0]_3+[2]_3 I, \quad [1]_3+[2]_3 I, \quad [2]_3+[2]_3 I\ \}. \end{aligned}$$

This is interesting because F is a field, but the number system we have already built with 9 elements, namely $\mathbb{Z}_9$, is *not* a field, since 9 is not prime. So F must be something fundamentally different to $\mathbb{Z}_9$.

(b) Each of the field laws aside from the multiplicative inverse law has a proof in F which is visually identical to the proof we gave earlier for it in $\mathbb{C}$. The only difference is that instead of the symbols a, b, etcetera denoting real numbers, they now denote elements of $\mathbb{Z}_3$. But $\mathbb{Z}_3$ is a field, so everything we did with them still works!

Here, then, is a proof of the left distributive law in F. I have *literally* copied and pasted it from the course notes, changing only a few symbols.

Let $z_1 = a_1 + b_1 I$, $z_2 = a_2 + b_2 I$, and $z_3 = a_3 + b_3 I$ be elements of F, so that $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}_3$. Now

$$\begin{aligned} z_1(z_2+z_3) &= (a_1+b_1 I)((a_2+a_3)+(b_2+b_3)I) \\ &= (a_1(a_2+a_3)-b_1(b_2+b_3))+a_1(b_2+b_3)+b_1(a_2+a_3))I, \end{aligned}$$

and

$$\begin{aligned} z_1z_2+z_1z_3 &= ((a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)I)+((a_1a_3-b_1b_3)+(a_1b_3+a_3b_1)I) \\ &= (a_1a_2-b_1b_2+a_1a_3-b_1b_3)+(a_1b_2+a_2b_1+a_1b_3+a_3b_1)I, \end{aligned}$$

and a little bit of rearranging, using the field laws in $\mathbb{Z}_3$, shows that the two expressions are the same.

(c) Again, this is like the complex numbers. This allows us to predict that the additive identity element will be $[0]_3+[0]_3I$. And indeed that satisfies the requisite equations: for any $z=a+bI$ in F, so that $a,b\in\mathbb{Z}_3$, we have

$$z+([0]_3+[0]_3I)=(a+bI)+([0]_3+[0]_3I)=(a+[0]_3)+(b+[0]_3)I=a+bI=z$$

and

$$([0]_3+[0]_3I)+z=([0]_3+[0]_3I)=(a+bI)=([0]_3+a)+([0]_3+b)I=a+bI=z$$

using in each line the definition of $+$ in F and then the additive identity law in $\mathbb{Z}_3$.

(d) Since F is finite, we could prove the multiplicative inverse law by brute force: write down the times table, and notice that every row other than the zero row contains the multiplicative identity element, which you can check is $[1]_3+[0]_3I$.

But there is a more conceptual way to do it. Recall that in the complex numbers, we had a formula for the multiplicative inverse that used the conjugate:

$$(a+b\mathrm{i})^{-1}=\frac{a-b\mathrm{i}}{a^2+b^2}.$$

This worked as long as a^2+b^2 was not zero, which it never was if $a+b\mathrm{i}$ was a nonzero complex number, because then one of a^2 or b^2 was positive and the other was nonnegative.

Does the same formula work in F? Well, we no longer have the notion "positive" to work with. But it turns out still to be true that $a^2+b^2=[0]_3$ if and only if $a=b=[0]_3$, for a and b elements of $\mathbb{Z}_3$! Why is this? Let's square all the elements of $\mathbb{Z}_3$:

$$([0]_3)^2=[0]_3, \qquad ([1]_3)^2=[1]_3, \qquad ([2]_3)^2=[1]_3.$$

The only way to get a sum of $[0]_3$ from two of these squares is if $a=b=[0]_3$; otherwise the sum is $[1]_3$ or $[2]_3$. So if $a+bI$ is nonzero, we can in fact define $(a+bI)^{-1}$ using the formula above. Let's check that it really is a multiplicative inverse:

$$\begin{aligned}(a+bI)\cdot\frac{a-bI}{a^2+b^2}=\frac{(a+bI)(a-bI)}{a^2+b^2}=\frac{(a^2+b^2)+[0]_3I}{a^2+b^2}= \\ =((a^2+b^2)+[0]_3I)(a^2+b^2)^{-1}=1.\end{aligned}$$

There is a subtle point in the above. It might look like circular reasoning that we are using the inverse $(a^2+b^2)^{-1}$ to define the inverse $(a+bI)^{-1}$. But the former inverse is computed in $\mathbb{Z}_3$, which is a subset of F since we should regard a and $a+[0]_3I$ to be the same for all $a\in\mathbb{Z}_3$. That is, $(a^2+b^2)+[0]_3I$ is just an element of $\mathbb{Z}_3$, and we know that elements of $\mathbb{Z}_3$ have multiplicative inverses, so this computation goes through.

(e) Yes, F can be interpreted this way. The ring I had in mind is

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} : a, b \in \mathbb{Z}\}.$$

with complex addition and multiplication. (Since $\mathbb{Z}[\mathrm{i}] \subseteq \mathbb{C}$, to check that $\mathbb{Z}[\mathrm{i}]$ is a ring with identity we need only check the closure laws, and that it contains the additive and multiplcative identity from $\mathbb{C}$ and is closed under additive inverses for $\mathbb{C}$.)

The equivalence relation is

$$R = \{(z, w) \in \mathbb{Z}[\mathrm{i}]^2 : w - z = 3v \text{ for some } v \in \mathbb{Z}[\mathrm{i}]\}.$$

I will leave it to you to check that if we work with classes $[a]_R$ instead of $[a]_3$ and let $I = [\mathrm{i}]_R$, then the definitions at the start of the question define the same functions as

$$[z]_R + [w]_R := [z + w]_R,$$
$$[z]_R \cdot [w]_R := [z \cdot w]_R.$$

For more questions on $\mathbb{Z}_m$, see the extra questions for Chapter 2.

For another question on a ring constructed in the same way as $\mathbb{Z}_m$ was, by defining operations $+$ and $\cdot$ on a set of congruence classes, see the extra questions on Chapter 4 (once I've posted them!) for a question about an equivalence relation on the ring $\mathbb{R}[x]$ of polynomials with real coefficients.

3.5 Properties of rings

Question 3.5.1 Let R be a ring with identity which does *not* satisfy the nontriviality axiom. Prove that R has only one element.

Solution Our assumption that R does not satisfy the nontriviality axiom implies that $0 = 1$ in R. Now for any element $x \in R$ we have

$$x = 1 \cdot x = 0 \cdot x = 0$$

using the multiplicative identity law and Proposition 3.13 from the notes. Therefore every element of R is equal to zero, i.e. zero is the only element of R.

Question 3.5.2

(a) Fill in the blank in the following assertion with the name of a kind of ring.

> Let R be a ________. Then the identity $x^2 - y^2 = (x + y) \cdot (x - y)$ is true for all x and y in R.

The kind of ring you name should have as few axioms as possible.

(b) Prove the assertion from part (a). Name the ring axiom or fact that you are using at each step of your proof.

When you're done, check which axioms you've used. Could you have named a more general kind of ring in part (a)?

Solution (b) To gain our bearings with the question, let's remember how to prove the equality $x^2 - y^2 = (x+y) \cdot (x-y)$ in a familiar setting, like the real numbers. This is just a matter of opening both brackets on the right hand side and following our nose:

$$\begin{aligned}(x+y)(x-y) &= x(x-y) + y(x-y) \\ &= xx + x(-y) + yx + y(-y) \\ &= x^2 - xy + yx - y^2 \\ &= x^2 - xy + xy - y^2 \qquad (*) \\ &= x^2 - y^2.\end{aligned}$$

Once we choose the correct set of axioms, this proof will still work in the context of rings.

(a) Now we consider which axioms we made use of in this proof. Several of them are merely ring axioms. Opening brackets is the distributive law, the last equality is the additive inverse law followed by the additive identity law to get rid of a "+0", and several uses of the additive associative law are hidden by the notation since I wasn't writing extra parentheses in sums of three or more terms. The reason I wrote the third equality out so pedantically was to foreground the fact that we have used the result of question 2; this result itself, however, can be proved using only the ring axioms. But there is one critical step, the fourth equality $(*)$, which uses the commutative law for multiplication.

As such, the proof above will work in any ring where the commutative law for multiplication holds. Thus the blank should be filled with $\boxed{\text{commutative ring}}$, and the above sequence of equalities is a proof valid whenever R is a commutative ring.

Commentary. The "right" way to argue that the assumption that R is commutative is essential would be to give a counterexample to the equation $x^2 - y^2 = (x+y) \cdot (x-y)$ in a non-commutative ring. The reason I didn't ask this is because we haven't properly studied any examples of non-commutative rings in lectures yet. But once we have – for instance, if you return to this question while you are revising for the exam – I encourage you to pick a non-commutative ring and think up such a counterexample.

Question 3.5.3 Let R be a ring with identity and a be an element of R such that $a^n = 0$ for some positive integer n. Prove that $1-a$ has a multiplicative inverse in R.

Solution This question is based on the formula for the sum of a geometric series. The key observation in that formula still works in any ring with identity.

A multiplicative inverse of $1-a$ is $1+a+\cdots+a^{n-1}$, since the distributive law, and the distributive-like properties of additive inverses (question 1 on the week 8 coursework sheet), imply

$$(1-a)(1+a+\cdots+a^{n-1}) = 1+a+\cdots+a^{n-1} - a - a^2 - \cdots - a^n = 1 - a^n = 1$$

and similarly

$$(1+a+\cdots+a^{n-1})(1-a) = 1 - a + a - a^2 + \cdots + a^{n-1} - a^n = 1 - a^n = 1.$$